FedRAMP® Secure Configuration Guide

for CGC, Inc.
(a Merlin Group Company)

Constellation GovCloud (CGC)

Version 1.0

March 1, 2026

How to contact us

For questions about Constellation GovCloud (CGC), or for questions about this document including how to use it, visit https://cgc.cloud/contact/

For more information about CGC, see https://cgc.cloud/

Secure Configuration Guide

Prepared for

Identification of Organization that Prepared this Document	
Organization Name	CGC, Inc., a Merlin Group Company
Street Address	1861 International Drive
Suite/Room/Building	Suite 500
City, State, Zip	McLean, VA 22102

Document Revision History

Date	Description	Version	Author
3/1/2026	Initial Draft	1.0	CGC

TABLE OF CONTENTS

1. Purpose

This Secure Configuration Guide (SCG) satisfies the FedRAMP Rev5 Balance Improvement Release requirement for secure configuration guidance applicable to enterprise-level administrative accounts and security settings.

This guide defines:

- Top-level administrative account protections
- Mandatory configuration safeguards
- Security implications of configuration decisions
- Operational and decommissioning requirements
- Customer and provider responsibility boundaries

This guidance applies to all CGC Landing Zones and associated SaaS application environments.

2. Scope

Constellation GovCloud (CGC) is a FedRAMP Moderate authorized General Support System (GSS) built on FedRAMP-authorized cloud infrastructure services. Each SaaS application hosted within CGC is deployed within a dedicated Landing Zone. This SCG governs enterprise-level administrative configuration controls within those environments.

3. Top-Level Administrative Accounts (Required)

3.1. Definition

Top-level administrative accounts are enterprise-scoped identities with unrestricted control over identity, policy, billing, guardrails, and global security configuration. Examples include:

- Platform Top-Level Administrative Account
- AWS GovCloud Root Account / Management Account
- Azure Global Administrator / Tenant Root
- GCP Organization Administrator

These accounts possess full authority over the enterprise cloud boundary.

3.2. Secure Access Requirements (Mandatory)

Top-level administrative accounts MUST:

- Enforce phishing-resistant, FIPS-validated MFA
- Prohibit shared credentials
- Be restricted via conditional access and IP allow listing

- Be used only for initial provisioning, break-glass, or account recovery
- Be monitored with security alerting for authentication, privilege, policy, and MFA changes
- Store credentials within FIPS-validated secure vault solutions

Security Implication: Compromise of a top-level administrative account enables enterprise-wide privilege escalation and bypass of guardrails.

3.3. Secure Configuration Responsibilities (Mandatory)

Top-level administrative accounts MUST:

- Configure and enforce RBAC across the enterprise
- Enforce least privilege and separation of duties
- Enable centralized audit logging and retention
- Configure encryption defaults for data at rest and in transit
- Establish and enforce organization-wide guardrails
- Configure backup and recovery protections
- Establish enterprise identity federation

Security Implication: Misconfiguration at the enterprise level may invalidate downstream compliance controls.

3.4. Secure Operations (Mandatory)

Top-level administrative accounts MUST:

- Never be used for routine operational workloads
- Be reviewed at least every 90 days for credential rotation and access validation
- Be continuously logged and integrated with centralized monitoring
- Be governed by documented break-glass procedures

Security Implication: Persistent operational use of enterprise administrative accounts increases compromise blast radius.

3.5. Decommissioning (Mandatory)

Upon decommissioning:

- Federation links MUST be removed
- Credentials MUST be rotated or invalidated
- Audit logs MUST be archived per retention requirements
- Subscription or project ownership MUST be formally transferred
- Delegated permissions MUST be verified and revoked

Security Implication: Failure to properly decommission may leave residual enterprise access.

4. Security Settings Restricted to Top-Level Administrative Accounts (Required)

The following controls may only be configured by top-level administrative accounts: Identity and Access

4.1. Federation configuration

- Cross-account trust relationships
- Enterprise RBAC baselines
- Conditional access policies

4.2. Organization Guardrails

- AWS Service Control Policies
- Azure Management Group Policies
- GCP Organization Policies

4.3. Logging and Monitoring

- Enterprise logging enablement
- Audit retention configuration
- Log export to secure storage

4.4. Encryption Controls

- Enforcement of FIPS-validated cryptography
- Enterprise key management configuration
- Customer-managed key enforcement

4.5. Billing and Governance

- Account or subscription creation
- Marketplace approvals

Security Implication: Improper modification of these controls can permit data exfiltration, privilege escalation, or compliance violation.

5. Privileged Accounts (Recommended Controls)

Privileged accounts have scoped administrative authority but do not control the enterprise boundary.

Recommended safeguards include:

- Segregation of duties across identity, network, security, and application roles
- Just-in-Time (JIT) privilege elevation
- Time-bound approvals
- Logged elevation activity

Security Implication: Persistent privileged access increases insider and credential compromise risk.

6. Logging and Monitoring Baseline

All administrative activity MUST:

- Be logged
- Be centrally retained
- Be immutable

Generate alerts for:

- Failed MFA attempts
- Privilege escalation
- Policy deletion
- Logging disablement

7. Customer Communication

This Secure Configuration Guide may be delivered via:

- Customer onboarding materials
- Documentation portals
- Security white papers
- API-accessible configuration baselines

All distributed formats MUST clearly define:

- Top-level administrative account naming
- Scope of authority
- Required protections
- Security implications

8. Responsibility Clarification

Determination of required FedRAMP impact level is the responsibility of the Agency Authorizing Official or designated security authority.

This SCG defines secure configuration safeguards within the CGC platform and does not determine agency-specific categorization requirements.